

AMENDMENT TO THE CLAIMS

Please amend claims 20-25 and 33, as follows:

At B1 don't
1 20. (Amended) A digital content encryption and decryption apparatus of a digital content
2 transmission system comprising:

3 a protocol format generator located at a server location, said protocol format generator
4 generating a copyright protection protocol in response to identity characters of a user transmitted to
5 said server location from a terminal unit, said copyright protection protocol including a header and
6 digital contents, said digital contents being encrypted, said header having information for decrypting
7 and explaining the digital contents; and

8 a protocol format decoder located at said terminal unit, said protocol format decoder having
9 a decryption algorithm, said protocol format decoder decrypting and replaying the digital contents
10 according to the information of the header received from the protocol format generator.

1 21. (Amended) The apparatus of claim 20, wherein the protocol format generator generates
2 a user key by adding key information to a key generation algorithm and calculates a hash value by
3 adding the user key to a hash algorithm, said protocol format generator encrypting a temporary
4 validation key by using the user key, said header including user authorization information with the
5 hash value and the encrypted temporary validation key, said key information being formed to
6 correspond to said identity characters of the user.

1 22. (Amended) The apparatus of claim 20, wherein the protocol format decoder generates
2 a user key by adding key information to a key generation algorithm and decrypts a temporary
3 validation key, transmitted within said copyright protection protocol, by using the user key, said
4 protocol format decoder decrypting the encrypted digital contents with the temporary validation key,
5 said key information being formed to correspond to said identity characters of the user.

23. (Amended) A digital content encryption and decryption apparatus of a digital content
transmission system comprising:

1 B1
2
3
4 a protocol format generator located at a server location, said protocol format generator
5 generating a copyright protection protocol by generating key information using random numbers,
6 said key information corresponding to identity characters of a user transmitted to said server location
7 from a terminal unit, said copyright protection protocol including a header and encrypted digital
8 information added to the header;

9 said protocol format generator applying said key information to a key generating algorithm
10 to generate a user key utilized to generate a temporary validation key, said temporary validation key
11 being encrypted to generate user authorization information, said header including said user
12 authorization information;

13 a protocol format decoder for copyright protection located at said terminal unit, said protocol
14 format decoder receiving and storing said key information and receiving said copyright protection
15 protocol; and

said protocol format decoder generating a second user key in response to the received key

16 information, analyzes said user authorization information in response to said second user key to
17 determine whether the terminal unit is authorized to receive said encrypted digital information, and
18 when said terminal unit is authorized to receive said encrypted digital information, utilizing said
19 second user key to decrypt said temporary validation key from said user authorization information,
20 the decrypted temporary validation key being used to decrypt said encrypted digital information.

B1
24. (Amended) The apparatus of claim 23, wherein the protocol format decoder generates
said second user key by adding the stored key information to a second key generation algorithm.

25. (Amended) A copyright protection protocol for protecting copyright of digital contents,
said protocol including a header and the digital contents, said digital contents being encrypted, said
header including key data for decrypting the digital contents, said key data being randomly generated
in response to identity characters of a user transmitted to a host server from a terminal unit, wherein
said terminal unit receives said protocol from said host server and replays said digital contents by
decrypting the encrypted digital contents in response to the key data.

33. (Amended) The protocol format of claim 27 or 28, wherein the encrypted header field
comprises a field for encryption algorithm of the digital content, a field for indicating a basic process
unit of the digital content, a field for indicating the number of encrypted byte, and a hash value field
for a hash value for determining a state of the entire header.